Cybercrime Legislation in the UK: Is the Computer Misuse Act 1990 Still Fit for Purpose?

Criminal Law & Cybersecurity Law

Difficulty	Advanced	**Recommended Length**	12,000 – 15,000 words
Keywords	Computer Misuse Act, cybercrime, UK law, ransomware, legislation, EU Cybercrime Directive	**Academic Support**	AssignProSolution.com

Introduction

The Computer Misuse Act 1990 was drafted when the internet barely existed as a public resource. It has been amended twice — in 1997 and 2006 — but the core framework remains largely as written. In the years since, cybercrime has become one of the most economically damaging categories of criminal activity in the UK, with ransomware attacks on critical infrastructure, AI-assisted fraud at scale, and state-sponsored intrusions that the 1990 Act was never designed to address. This dissertation asks the direct question: does the legislation still work?

Background and Context

The CMA 1990 created three main offences: unauthorised access, unauthorised access with intent to commit further offences, and unauthorised modification of computer material. These categories were adequate for the threat environment of the early 1990s. They are significantly less adequate for ransomware-as-a-service operations run from foreign jurisdictions, phishing infrastructure hosted across multiple legal territories, or deepfake fraud that does not involve 'modification' in the traditional sense. The Law Commission reviewed the Act in 2020 and recommended updates that have not yet been implemented.

Key Research Questions

1. Does the CMA 1990 adequately criminalise contemporary cybercrime vectors including ransomware, phishing, and AI-assisted fraud?
2. How does the UK's cybercrime legislation compare with the EU Cybercrime Directive (2013/40/EU) and the Budapest Convention?
3. What are the practical enforcement challenges and how does jurisdictional fragmentation undermine prosecution?
4. What legislative reforms would produce a more effective legal framework without overcriminalising legitimate security research?

Suggested Methodology

Doctrinal legal analysis of the CMA 1990 and its amendments, combined with comparative legal analysis against EU and international frameworks. Case law review drawing on CPS prosecution data and appeal court decisions. Policy document analysis from the Law Commission, NCSC, and Home Office. A small number of practitioner interviews (cybercrime lawyers, Crown Prosecution Service lawyers, or NCSC policy staff) adds valuable primary data if access can be arranged.

Key Theoretical Frameworks

- Hart's Concept of Law — rule of recognition, primary and secondary rules
- Deterrence Theory in criminal law — Bentham; Becker (1968)
- Legal Positivism vs Natural Law in technology regulation
- Comparative law methodology — Zweigert & Kötz (1998)

Common Challenges and How to Address Them

The pace of technological change makes any legal analysis risk feeling dated before submission. Build in a clear scope statement — 'this dissertation analyses the legal framework as it stood at [date]' — and focus the analytical contribution on the structural gaps in the legislation rather than cataloguing specific recent attacks, which dates quickly.

Conclusion and Next Steps

This is a dissertation topic with genuine policy relevance at a moment when the Home Office is actively reconsidering the UK's cybercrime framework. A strong piece here can make a real contribution to the debate rather than simply summarising existing positions. If you need support developing the comparative law sections or structuring the legal argument, **AssignProSolution.com** offers specialist academic writing assistance.

Need expert help with this dissertation? Get professional academic writing support at **AssignProSolution.com** — proposals, chapter plans, full dissertations, and editing.

© 2025 AssignProSolution.com — For academic reference and inspiration.